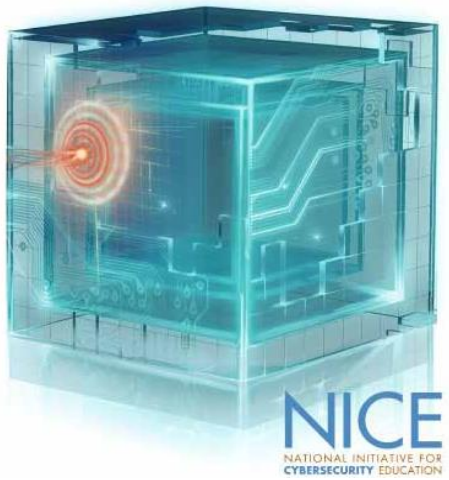
Homeland Security

THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

USER GUIDE–

Employers



Workforce Framework User Guide

Welcome to the User Guide!

The Workforce Framework helps **Employers** to recruit from a larger pool of more qualified candidates.

The National Initiative for Cybersecurity Education (NICE) developed the National Cybersecurity Workforce Framework to categorize and define cybersecurity work.

When degrees, jobs, training and certifications are aligned to the Workforce Framework...
Colleges & Training Vendors can create programs that are aligned to jobs
Students will graduate with knowledge and skills that employers need
Employers can recruit from a larger pool of more qualified candidates
Employees will have a better defined career path and opportunities
Policy Makers can set standards to evolve the field

Workforce Framework User Guide

What's in this User Guide?

This guide was created to help you and your organization use the Workforce Framework. As you navigate through the guide, you will find:

- A Workforce Framework Overview.
- Benefits of implementing the Workforce Framework within your company/organization.
- Recommended steps for implementation.
- Useful tools and links that will help you promote and use the Workforce Framework.

The National Cybersecurity Workforce Framework

Led by the Department of Homeland Security (DHS), the National Initiative for Cybersecurity Education (NICE) raises public awareness, provides a foundation for the recruitment, training, and retention of cybersecurity professionals, and promotes cybersecurity education. The Workforce Framework (in support of the "Evolve the Field" goal) is a national resource providing employers, educators, trainers, and policy makers a common language for describing cybersecurity work.

The Workforce Framework contains cybersecurity Specialty Areas, knowledge, skills, and abilities (KSAs), tasks, and sample job titles. It has been updated to reflect the evolving cybersecurity field and incorporate diverse viewpoints across government, industry, and academia. Explore the Workforce Framework at the National Initiative for Cybersecurity Careers and Studies (NICCS™) website.

The Workforce Framework is:

A Blueprint

- Describes and categorizes cybersecurity work.
- Identifies sample job titles, tasks, and knowledge, skills, and abilities (KSAs).

A Tool

- Provides a foundation organizations can use to develop position descriptions, competency models, and training.

A Collaboration

- Incorporates inputs from industry, academia, and government.
- Addresses the nation's need to identify, qualify, and develop the cybersecurity workforce.

Using the Workforce Framework – Employers

Having a common framework for describing cybersecurity work allows ***Employers*** to develop job descriptions that reflect critical knowledge and skills, tasks, and roles/responsibilities using consistent cybersecurity language.

Using the Workforce Framework, Employers can:

- Support the nation's cybersecurity workforce development efforts.
- Build a foundation for developing position descriptions, designing competency models, and creating training.
- Understand the key KSAs cybersecurity professionals should possess, which can help develop strategies for attracting the best and brightest talent.
- Determine workforce capabilities in cybersecurity.

Using the Workforce Framework, Federal Government Employers can:

- Align to Federal Government workforce development products (e.g., Department of Labor (DOL) cybersecurity competency model, Federal Chief Information Officer (CIO) Council cybersecurity roles, Office of Personnel Management (OPM) eHRIS data element*, and others).

* The Office of Personnel Management's (OPM) Cybersecurity Data Element Standard provides a set of data element codes as a position classification tool. These data element codes are aligned to the Workforce Framework and are required be coded to any positions performing cybersecurity work. Click here for more information on the OPM Data Element and its required use for Federal Departments and Agencies

Why is the Workforce Framework Important?

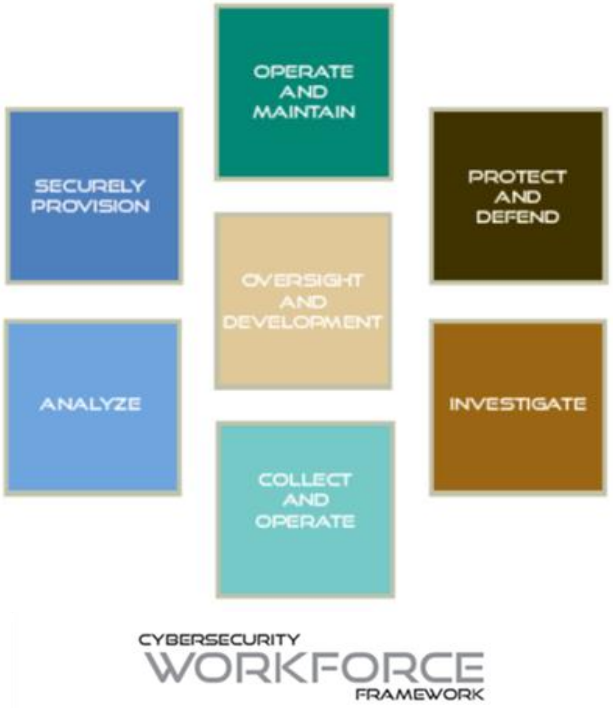
The Workforce Framework categorizes cybersecurity work and identifies cybersecurity Specialty Areas.

The Workforce Framework establishes:

- A common taxonomy and language which organizes cybersecurity work into seven Categories and more than 30 Specialty Areas.
- A baseline of tasks, Specialty Areas, and KSAs associated with cybersecurity professionals.

The Workforce Framework improves our Nation's ability to:

- Provide employers, educators, trainers, and policy makers a common language for describing cybersecurity work.
- Build and maintain the highly skilled and agile workforce needed to protect the nation.
- Coordinate and collectively address cybersecurity threats.



What are the Seven Categories?

The Workforce Framework's Categories organize Specialty Areas by grouping similar work.

Securely Provision	Specialty Areas concerned with conceptualizing, designing, and building secure IT systems.
Operate and Maintain	Specialty Areas responsible for providing the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security.
Protect and Defend	Specialty Areas responsible for identifying, analyzing, and mitigating threats to IT systems.
Investigate	Specialty Areas responsible for the investigation of cyber events or crimes which occur within IT Systems and networks.
Collect and Operate	Specialty Areas responsible for the highly specialized and largely classified collection of cybersecurity information that may be used to develop intelligence.
Analyze	Specialty Area responsible for highly specialized and largely classified review and evaluation of incoming cybersecurity information.
Oversight and Development	Specialty Areas that provide critical support so others may conduct their cybersecurity work.

What are the Specialty Areas?

Specialty Areas describe a cybersecurity work area, or function. Each Specialty Area includes related Tasks, KSAs, and sample job titles.

Securely Provision
- Technology Research and Development
- Systems Requirements Planning
- Systems Security Architecture
- Software Assurance and Security Engineering
- Systems Development
- Test and Evaluation
- Information Assurance (IA) Compliance

Analyze
- Cyber Threat Analysis
- All Source Intelligence
- Targets
- Exploitation Analysis

Collect and Operate
- Operations Planning
- Cyber Operations
- Collection Operations

Protect and Defend
- Computer Network Defense (CND) Analysis
- Vulnerability Assessment and Management
- Incident Response
- Computer Network Defense (CND) Infrastructure Support

Investigate
- Investigation
- Digital Forensics

Oversight and Development
- Strategic Planning and Policy Development
- Security Program Management (CISO)
- Information Systems Security Operations (ISSO)
- Education and Training
- Legal Advice and Advocacy

Operate and Maintain
- System Administration
- Network Services
- Customer Service and Technical Support
- Systems Security Analysis
- Data Administration
- Knowledge Management

National Initiative for Cybersecurity Careers and Studies (NICCS™)

For more information on the Workforce Framework, visit National Initiative for Cybersecurity Careers and Studies (NICCS™) website. NICCS is the one stop shop for cybersecurity careers and studies. There, you will find a wealth of information on the Workforce Framework. The site also connects you with information on:

- Cybersecurity Awareness
- Professional Certifications and Courses
- Academic and Hands-on Learning Opportunities
- Workforce Development Strategies
- Federal Cybersecurity Training Events (FedCTE)
- Federal Virtual Training Environment (FedVTE)

Visit NICCS: www.niccs.us-cert.gov/

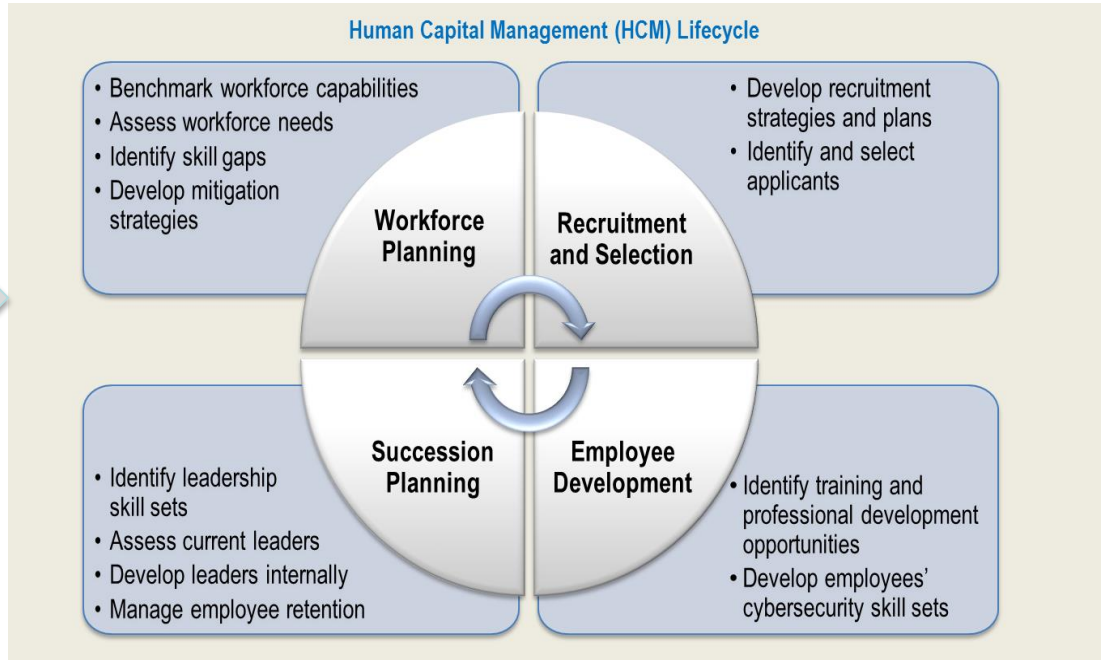
Benefits of using the Workforce Framework

The Workforce Framework benefits ***Employers*** by defining cybersecurity functions and creating a common taxonomy which can be used when referring to cybersecurity work. This is done irrespective of organizational structures, job titles, or other individual conventions. The Workforce Framework:

- ✓ Provides consistent language organizations can use to describe and define their cybersecurity workforces**.**
- ✓ Supports skill assessment and gap identification to identify training needed to develop and maintain a high-performing workforce.
- ✓ Aids in the classification of workers into common cybersecurity roles, which can help streamline workforce development efforts.
- ✓ Supports workforce planning activities and helps managers assess the critical cybersecurity job roles in their organizations.
- ✓ Helps Employers identify workload supply and demand needs, adapt recruitment and selection procedures and/or develop training programs that support KSA development.
- ✓ Helps Federal Departments and Agencies respond to mandates and surveys*.

Implementing the Workforce Framework Within Your Organization

The Workforce Framework enhances understanding of cybersecurity work, creates consistency, and can be used to inform Human Capital Management (HCM) Lifecycle activities.



How can you use the Workforce Framework?

The Workforce Framework's taxonomy can be used to standardize common cybersecurity work areas, tasks, KSAs, and recommended job titles. The content can be customized for specific organizations or remain general for broader audiences. Since the size and capabilities of cybersecurity workforces vary by organization, different methods of adopting the Workforce Framework can be applied.

The recommended process below can help your organization adopt the Workforce Framework.

STEP 1

Define Cybersecurity Roles
Assess your cybersecurity workforce and ensure your roles are consistent with the Workforce Framework.

STEP 2

Develop Cybersecurity Competency Models
Once you define your organization's cybersecurity roles, develop competency models.
**Federal guidance requires Federal Departments and Agencies to develop competency models for employees.

STEP 3

Conduct Workforce Planning
Use your newly defined cybersecurity roles to gather and assess data for workforce planning efforts.

STEP 4

Plan for the Future
Using the data from Steps 1 – 3, develop additional workforce development strategies (e.g., recruitment, selection, succession planning, and training development).

STEP 1: Define Cybersecurity Roles

The first step is to define your organization's cybersecurity roles. You can either adopt general/pre-defined roles, or develop your own customized, roles.

General Cybersecurity Roles

- Recommended for organizations with limited resources for role development, or those with cybersecurity duties.
- Employer example: The Federal Chief Information Officers Council (CIOC) developed 13 roles to demonstrate this application. Those roles are in this guide.

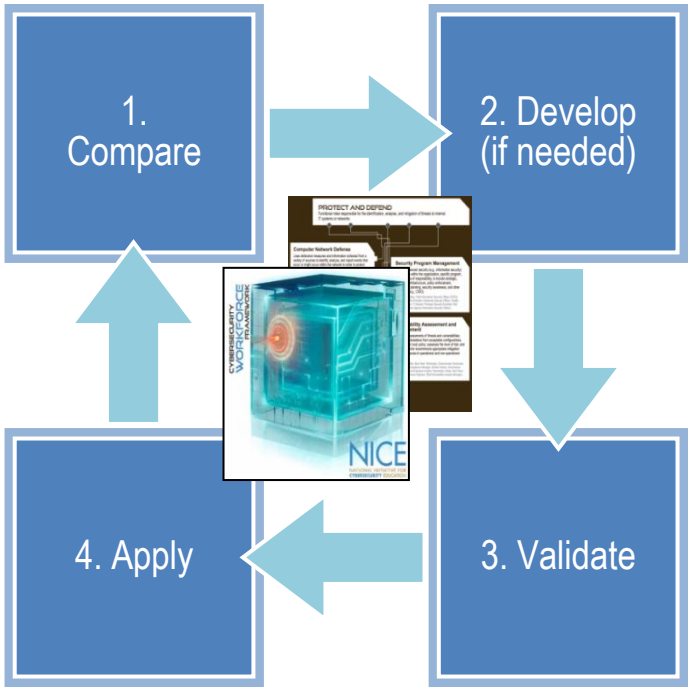
Customized Cybersecurity Roles

- Recommended for organizations with resources available to develop cybersecurity roles, or those with many unique or specialized cybersecurity roles.
- Defines specialized cybersecurity roles and identifies role-specific competencies.

Role Definition Process

Here is a recommended process for defining your organization's cybersecurity roles:

1. **COMPARE the roles used by your organization to the general roles.**
   - Conduct a review (using Subject Matter Experts or (SMEs)) of your organization's current cybersecurity roles. Compare your roles with the Workforce Framework examples.
2. **DEVELOP cybersecurity roles (if needed).**
   - If your current roles do not match the Workforce Framework examples, customize the examples or create new roles to meet your organization's needs.
3. **VALIDATE the role's definitions, tasks, and KSAs.**
   - Review and validate with SMEs to ensure that the definitions, tasks, and KSAs are applicable to your organization's needs.
4. **APPLY the Workforce Framework to other workforce development activities.**
   - Utilize the Workforce Framework content for other efforts (e.g., recruitment, selection, succession planning, and training development).



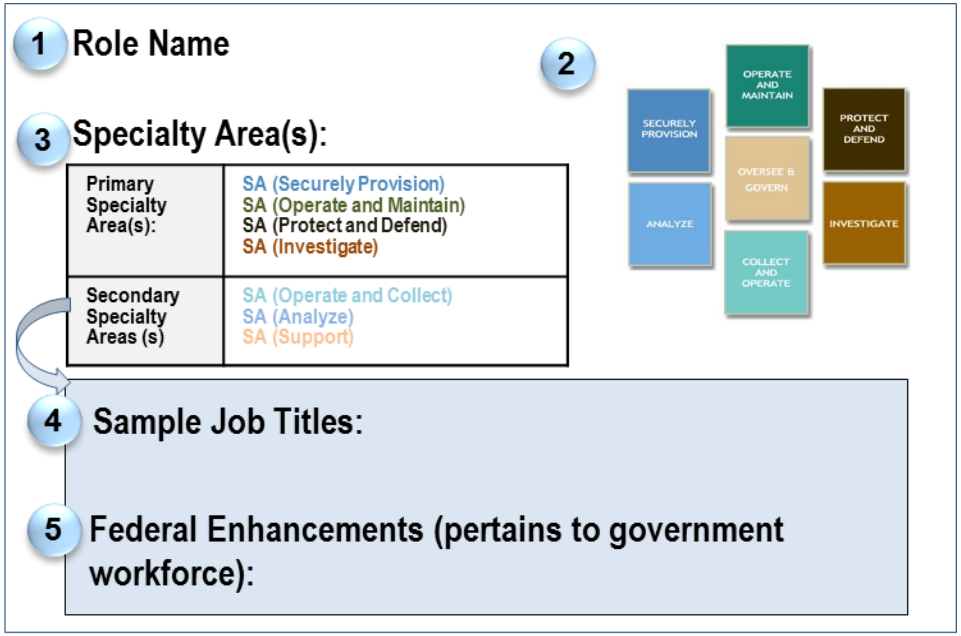
General Cybersecurity Roles

If your organization has a limited number or type of cybersecurity positions, you may prefer to choose the general roles*. **There are 13 Workforce Framework-based streamlined cybersecurity roles to promote consistency and standardization of the cybersecurity workforce.**

Each role consists of sample job titles and definition, the related Workforce Framework Category, and the Workforce Framework Specialty Areas.

Sample Cybersecurity Role Template

1. **Role Name**
2. **Framework Category**
3. **Framework Specialty Area**
4. **Sample Job Titles**
5. **Federal Enhancements, if any**



Click the links below to view each general role.*

- Systems Operations Professional
- Data Administrator
- Computer Network Defense (CND) Specialist
- Digital Forensics and Incident Response Analyst
- Information Security Auditor
- Information Systems Security Officer
- Information Systems Security Manager
- Information Security Architect
- Risk and Vulnerability Analyst
- Software Developer
- Information Systems Security Engineer
- Strategic Planning and Policy Development Professional
- Chief Information Security Officer (CISO)

*General roles developed by the Federal Chief Information

Customized Cybersecurity Roles

If your organization has unique or specialized positions, you may choose to develop customized cybersecurity roles.

The template below can be used to build customized cybersecurity roles as needed.

Role Name	[Fill in Role Name]
Prominent Workforce Framework Specialty Areas	• Specialty Area 1 • Specialty Area 2 • [Fill in other Specialty Areas]

Role Definition: [Define the role here. Be sure to include any organization-specific job duties.]

STEP 2: Develop Cybersecurity Competency Models

In step two, role-specific competency models for cybersecurity professionals can be developed.

Competency models helps organizations:

- ✓ Establish a baseline of role-specific cybersecurity competencies, which can help determine capability requirements for cybersecurity roles.
- ✓ Provide parameters for building an effective, mission-focused cybersecurity workforce.
- ✓ Assess skills, identify skills gaps, and determine workforce training needs.
- ✓ Build competency across the organization and create a more comprehensive and structured approach to workforce development.

What is a Competency Model?

Competencies are individual or organizational attributes required for successful performance within a role or position. Competencies describe workforce characteristics and behaviors individuals must exhibit to successfully perform their specific role. Technical competencies are unique to a specific role and distinguish it from others. Technical competencies are most useful for identifying capabilities in mission critical roles.

A competency model typically includes the following elements:

1. **Competency titles**
2. **Competency definitions -** to describe the type of work and the context of the role.
3. **Behavioral indicators** (BIs) describing an individual's proficiency level how the competencies manifest themselves in on-the-job behaviors. BIs typically increase in scope, complexity, and responsibility at higher levels of proficiency.
4. **Proficiency targets** identifies the level of proficiency required to perform successfully within a particular role or occupation.

DECISION MAKING (1)	Makes sound, well-informed, timely, and objective decisions; perceives the impact and implications of decisions; commits to action, even in uncertain situat(2), to accomplish organizational goals		
BEHAVIORAL INDICATORS			
1 – BASIC	2 – INTERMEDIATE	3 - ADVANCED	4 – EXPERT
▪ Makes sound and timely decisions involving simple or routine situations ▪ Recognizes situations and limitations when further guidance is needed from a senior colleagues or supervisor	▪ Makes effective decisions involving moderately complex issues affecting(3) organization's functions and operations ▪ Prioritizes own work assignments in accordance with guidance provided by supervisors and stated project requirements	▪ Participates in analyzing, evaluating, and making recommendations improving programs or procedures ▪ Regularly evaluates the effectiveness of decisions made compared to stated objectives and adjusts future decisions as appropriate	▪ Makes sound and timely decisions involving multiple complex issues impacting the work and outcomes across multiple organizations ▪ Defines and clarifies complex issues and evaluates alternatives to select the optimal course when multiple courses of action are possible

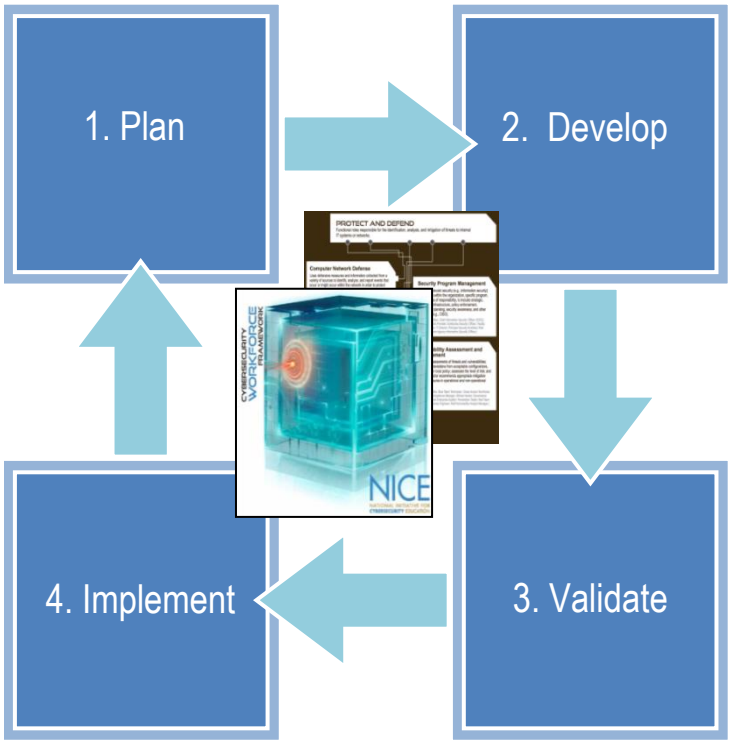
Illustrative

GRADE	(4) TARGET PROFICIENCY
GS-13	BASIC/ IINTERMEDIATE
GS-14	ADVANCED
GS-15	EXPERT

Competency Model Development Process

Here is a recommended high level approach to developing a cybersecurity competency model:

1. **PLAN and prepare for the competency development project**
   - Determine objectives, methodology, key activities and milestones with organization leadership and project team.
   - Identify the organizational cybersecurity roles to be modeled.
   - Identify Subject Matter Experts (SMEs) and engage key stakeholders.
2. **DEVELOP competency model.**
   - Review existing competency model information
   - Collect data (e.g., document review, focus groups); identify competencies, behavioral indicators (BIs), and proficiency targets.
   - Develop draft competencies and competency model(s).
3. **VALIDATE competency model with leadership and SMEs.**
   - Review and validate with SMEs and leadership to ensure competencies and models are applicable and align to organizational needs.
4. **IMPLEMENT competency model.**
   - Utilize the competencies and competency models for other efforts (e.g., recruitment, selection, succession planning, and training development).

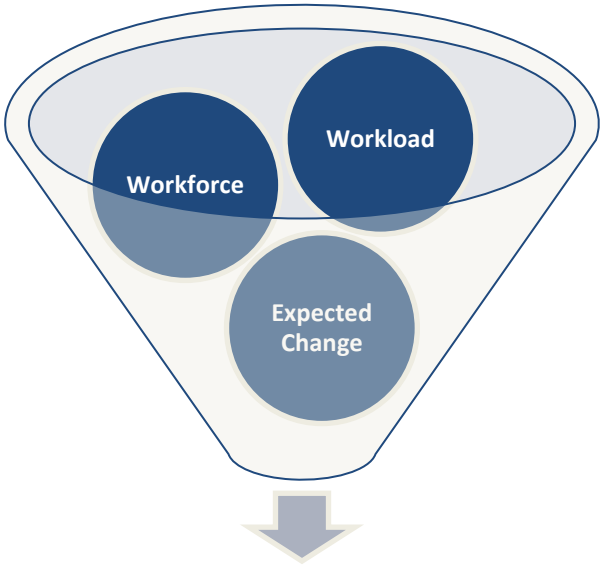


STEP 3: Conduct Workforce Planning

As the demands of global business, computing, and society revolve around information technology, cybersecurity workload is increasing faster than cybersecurity professionals can meet the demand. As such, an emerging priority in cybersecurity is the question of how organizations track, assess, grow, and shape this specialized workforce.

Workforce planning is the process organizations can use to address these concerns. It analyzes demand issues and helps organizations close the workforce gap in a systematic way.

- **Workforce Planning helps answer:**
  - What does our current workforce look like?
  - How many cybersecurity workers do we have?
  - What positions do these individuals hold?
  - What is their current workload?
- **Workforce Planning helps plan for the future:**
  - Do we anticipate changes in workload?
  - Are our workers correctly aligned to the work?
  - What competencies should the position require based on the workload?
  - Is additional training needed if the work is changing?
  - Are new positions needed?
  - Do we have the budget to fund the positions needed to meet our goals and objectives?



Workforce Planning and Analysis

What is Workforce Planning?

Effective workforce planning highlights potential risk areas associated with aligning workforce to work. Applied correctly, workforce planning allows organizations to adjust resources to meet future workloads, patterns of work, and fundamental changes in how work is accomplished. The approach must fit the needs of a specific organization and account for unique characteristics of the cybersecurity profession.

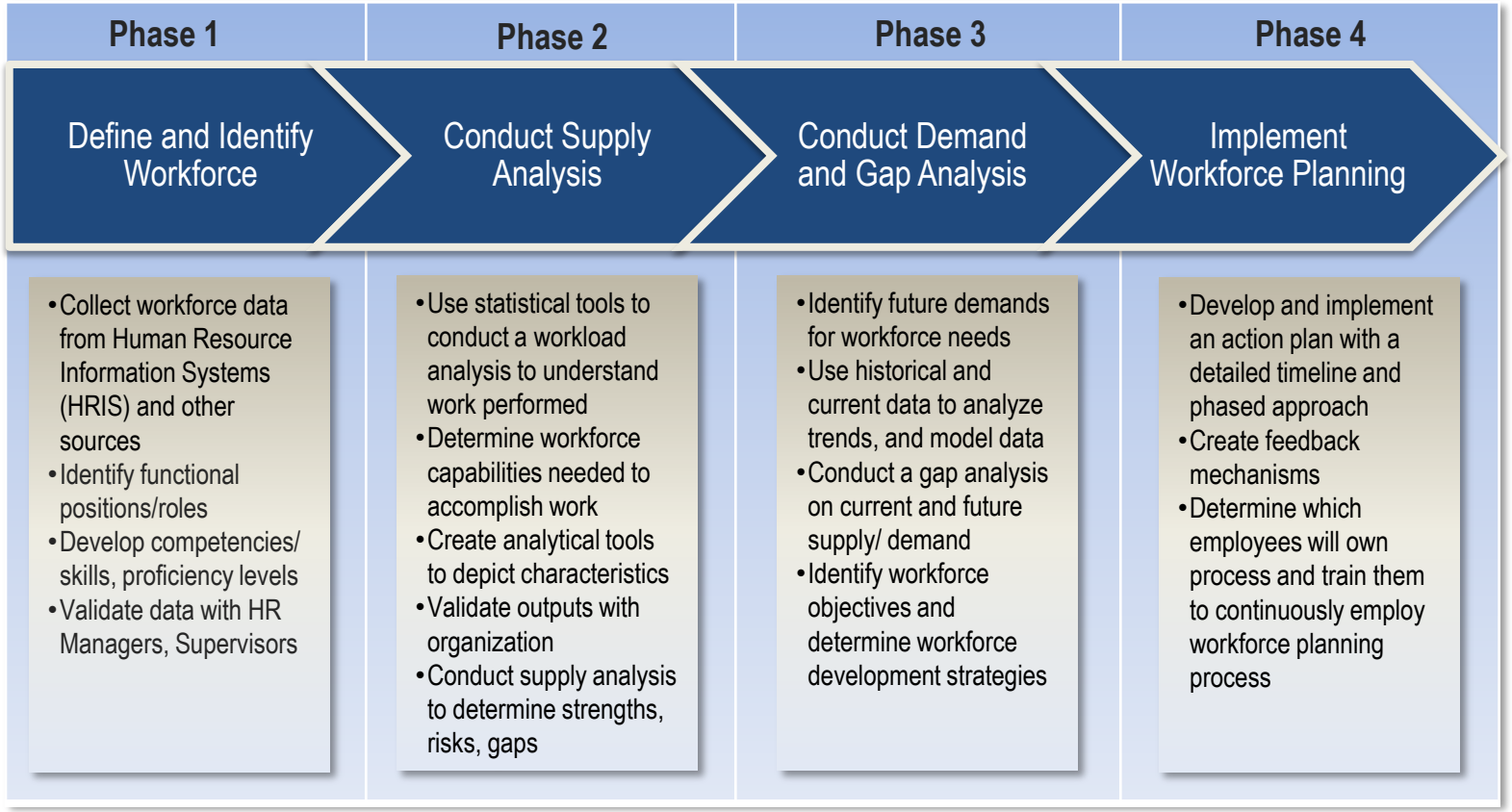
Workforce planning consists of three components:

- **Process:** An integrated and consistent means of diagnosing workforce needs and risks. This includes a defined model, data and analytics.
- **Strategy:** A direct line of sight between business and workforce requirements. This includes a shared vision, governance, and continuous monitoring or performance.
- **Infrastructure:** An effective and repeatable workforce planning process. This includes a healthy workforce or people, collaboration across levels and enabling technology.

A **workforce planning process,** identifies and quantifies the workload and workforce requirements unique to an organization; and analyzes the skills needed to fill the gap in workforce.

Workforce Planning Process

Using a Workforce Planning Process, such as the example provided below, an organization can conduct a cybersecurity workforce and workload analysis, enabling it to identify current and future needs and potential gaps which may impact an organization's ability to meet goals and objectives.



Workforce Planning White Papers

NICE developed two White Papers addressing the need of Workforce Planning within the cybersecurity field and to make recommendations on how to conduct workforce planning within this field.

Best Practices for Cybersecurity Workforce Planning White Paper

This paper reviews workforce planning methodologies for cybersecurity, and guidance for organizations. It synthesizes best practices from over 70 Federal organizations, interviews, workforce planning benchmarking studies, Federal reports, and workforce planning guides, and organized across three best practice components — process, strategy, and infrastructure.

Cybersecurity Capability Maturity Model (CMM) White Paper

This paper introduces a qualitative management tool, a Cybersecurity Workforce Planning CMM, to help organizations apply the elements of best practice workforce planning to analyze their cybersecurity workforce requirements and needs. The CMM provides a structure for organizations to baseline current capabilities in cybersecurity workforce planning, and enables leaders to make better decisions about how to support progression and what investments to make in regard to cybersecurity human capital initiatives.

Workforce Planning Diagnostic Tool

The Workforce Planning Diagnostic tool (the Diagnostic) intended to supplement and build upon previous national workforce planning efforts related to the Workforce Framework.

Using the concepts of risk exposure and risk tolerance, the Diagnostic helps organizations determine the types of organizational data necessary to execute their cybersecurity workforce planning process.

The **Cybersecurity Workforce Planning Diagnostic Tool** provides organizations with:

1. A qualitative tool to identify cybersecurity risk exposure and willingness to take on greater cybersecurity risk (risk tolerance) due to the nature of the organization and the types of activities in which it engages.
2. Placement within a quadrant aligning to one of four potential risk exposure/risk tolerance types: low risk/low tolerance; high risk/high tolerance; high risk/low tolerance; and low risk/high tolerance. (After completing the Diagnostic, organizations can tally their combined risk exposure and risk tolerance score, and subsequently place themselves into a risk exposure/risk tolerance quadrant).
3. Specific guidelines on the type of data an organization needs to collect to perform effective cybersecurity workforce planning processes (e.g., analyze gaps and identify future workforce needs) based on the risk exposure/risk tolerance type.

STEP 4: Plan for the Future

Once you have defined your organization's roles, developed competency models, and conducted other workforce planning activities (e.g., supply and demand analysis), you will have relevant workforce information that can drive your cybersecurity workforce development decision making

More information will be available on the **National Institute for Cybersecurity Studies (NICCS)** website, linking you to other Workforce Development efforts supported by the National Cybersecurity Workforce Framework.

Within the NICCS website, you will find additional information on:

- Training- Search for cybersecurity training and certification courses (mapped to the Workforce Framework)
- Professional Development- Discover how to plan your cybersecurity career
- Workforce Planning- Use tools and guidance to help improve your organization's cybersecurity workforce

Contact Us

This is the end of the Workforce Framework user guide for EMPLOYERS.

To learn more about the Workforce Framework and other Cybersecurity Education and Awareness (CE&A) Programs please contact:

Robin "Montana" Williams
Branch Chief, DHS Cybersecurity Education & Awareness
Phone: (703) 235-5169
Email: robin.williams@hq.dhs.gov

Kristina Dorville
Deputy Branch Chief, DHS Cybersecurity Education & Awareness
Phone: (703) 235-5281
Email: kristina.dorville@hq.dhs.gov

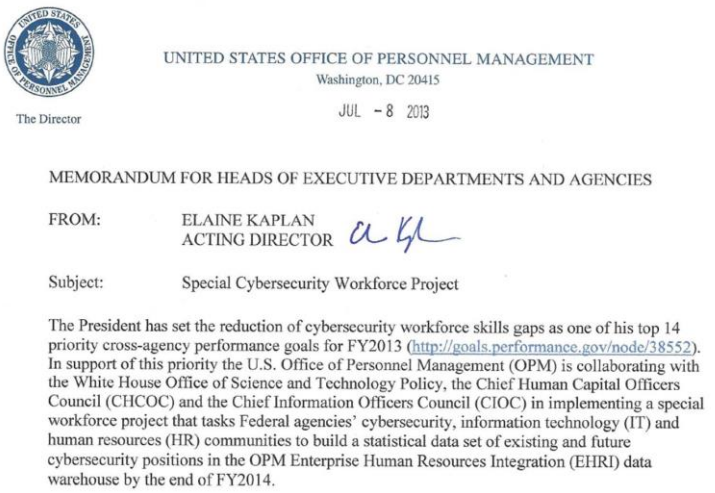
What is the OPM Data Element?

The OPM Data Elements are derived directly from the Workforce Framework's Categories and Specialty Areas. The July 8, 2013 OPM Data Element Memo requires US federal departments and agencies to track cybersecurity positions using the Workforce Framework.

Selection of a Data Element (or a Cybersecurity Category or Specialty Area) should be based upon the duties in which the incumbent is primarily engaged or which best reflects the requirements of the job.

Key points to using the OPM Data Element include:

- ✓ Only one code is permitted so it is important that the most appropriate code is used and that the codes are used consistently.
- ✓ If the work of an incumbent or the requirements of a position are predominantly in one Specialty Area, that code should be used.
- ✓ If there are multiple relevant Specialty Areas within a Category and no single Specialty Area predominated, the code for the Category in which those Specialty Areas fall should be used.



The Director

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

JUL - 8 2013

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: ELAINE KAPLAN
ACTING DIRECTOR

Subject: Special Cybersecurity Workforce Project

The President has set the reduction of cybersecurity workforce skills gaps as one of his top 14 priority cross-agency performance goals for FY2013 (http://goals.performance.gov/node/38552). In support of this priority the U.S. Office of Personnel Management (OPM) is collaborating with the White House Office of Science and Technology Policy, the Chief Human Capital Officers Council (CHCOC) and the Chief Information Officers Council (CIOC) in implementing a special workforce project that tasks Federal agencies' cybersecurity, information technology (IT) and human resources (HR) communities to build a statistical data set of existing and future cybersecurity positions in the OPM Enterprise Human Resources Integration (EHRI) data warehouse by the end of FY2014.

How do I use the OPM Data Element?

OPM has developed data standards, or data elements, to facilitate the use of Federal civilian human resources data. The standards also help avoid unnecessary duplication and incompatibility in the collection, process, and dissemination of such data.

OPM will require agencies to utilize cybersecurity codes specifically developed to identify these positions across occupational series in the Enterprise Human Resources Integration (EHRI) status and dynamic submissions. The usual timeframe allowed to service providers varies from 9 – 18 months to reprogram their systems. Once the programming is completed, and agencies are able to submit data in EHRI, then reports can be requested from the OPM Data Analysis group. The data element standards satisfy information needs, are maintained by human resources professionals, and coordinated by the Office of the Chief Information Officer.

The OPM Data element will:

- ✓ Identify positions for which the primary function is cybersecurity.
- ✓ Enable OPM and Federal agencies to identify the cybersecurity workforce, determine baseline capabilities, examine hiring trends, identify skill gaps, and more effectively recruit, hire, train, develop and retain an effective cybersecurity workforce.
- ✓ Allow HR Professionals to better understand their workforce and what issues need to be addressed.

OPM Data Elements

The OPM Cybersecurity Data Elements are in the tables on the following pages.

Code	Category/Specialty Area Label and Definition
00	**Not Applicable** - Position does not involve work in one or more cybersecurity functions.
10	**Analyze** - Specialty areas responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
11	**All Source Intelligence** - Analyzes threat information from multiple sources, disciplines, and agencies across the Intelligence Community. Synthesizes and places information in context; draws insights about the possible implications.
12	**Exploitation Analysis** - Analyzes collected information to identify vulnerabilities and potential for exploitation.
13	**Targets** - Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.
14	**Threat Analysis** - Identifies and assesses the capabilities and activities of cyber criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.
20	**Investigate** - Specialty areas responsible for investigation of cyber events and/or crimes of information technology (IT) systems, networks, and digital evidence.
21	**Digital Forensics** - Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.
22	**Investigation** - Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include but not limited to interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.
30	**Collect and Operate** - Specialty areas responsible for specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
31	**Collection Operations** - Executes collection using appropriate strategies and within the priorities established through the collection management process.

OPM Data Elements (continued)

Code	Category/Specialty Area Label and Definition
32	**Cyber Operations** - Performs activities to gather evidence on criminal or foreign intelligence entities in order to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.
33	**Cyber Operations Planning** - Performs in-depth joint targeting and cyber planning process. Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations.
40	**Operate and Maintain** - Specialty areas responsible for providing support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
41	**Customer Service and Technical Support** - Addresses problems and installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support).
42	**Data Administration** - Develops and administers databases and/or data management systems that allow for the storage, query, and utilization of data.
43	**Knowledge Management** - Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.
44	**Network Services** - Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.
45	**System Administration** - Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Also manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.
46	**Systems Security Analysis** - Conducts the integration/testing, operations, and maintenance of systems security.

OPM Data Elements (continued)

Code	Category/Specialty Area Label and Definition
50	**Protect and Defend** - Specialty areas responsible for identification, analysis, and mitigation of threats to internal information technology (IT) systems or networks.
51	**Computer Network Defense (CND) Analysis** - Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.
52	**Computer Network Defense (CND) Infrastructure Support** - Tests, implements, deploys, maintains, reviews and administers the infrastructure hardware and software that are required to effectively manage the computer network defense (CND) service provider network and resources. Monitors network to actively remediate unauthorized activities.
53	**Incident Response** - Responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.
54	**Vulnerability Assessment and Management** - Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations or enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.
60	**Securely Provision** - Specialty areas responsible for conceptualizing, designing, and building secure information technology (IT) systems (i.e., responsible for some aspect of systems development).
61	**Information Assurance (IA) Compliance** - Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new information technology (IT) systems meet the organization's information assurance (IA) and security requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.
62	**Software Assurance and Security Engineering** - Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.

OPM Data Elements (continued)

Code	Category/Specialty Area Label and Definition
63	**Systems Development** - Works on the development phases of the systems development lifecycle.
64	**Systems Requirements Planning** - Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.
65	**Systems Security Architecture** - Develops system concepts and works on the capabilities phases of the systems development lifecycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.
66	**Technology Research and Development** - Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.
67	**Test and Evaluation** - Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of elements of systems incorporating IT.
70	**Oversight and Development** - Specialty areas providing leadership, management, direction, and/or development and advocacy so that individuals and organizations may effectively conduct cybersecurity work.
71	**Education and Training** - Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers, and/or evaluates training courses, methods, and techniques as appropriate.
72	**Information Systems Security Operations (Information Systems Security Officer [ISSO])** - Oversees the information assurance (IA) program of an information system in or outside the network environment; may include procurement duties.
73	**Legal Advice and Advocacy** - Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.

OPM Data Elements (continued)

Code	Category/Specialty Area Label and Definition
74	**Security Program Management (Chief Information Security Officer [CISO])** - Manages information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources.
75	**Strategic Planning and Policy Development** - Applies knowledge of priorities to define an entity's direction, determine how to allocate resources, and identify programs or infrastructure that are required to achieve desired goals within domain of interest. Develops policy or advocates for changes in policy that will support new initiatives or required changes/enhancements.
80	**Cybersecurity Program/Project Management** - Manages one or more cybersecurity project(s) or program(s) to provide products and/or services. Coordinates, communicates and integrates cybersecurity projects and program activities. Ensures cybersecurity work efforts achieve the intended or specified outcomes. May encompass the decision-making and negotiation responsibilities involved in executing the program efforts.
90	**Cybersecurity Supervision, Management, and Leadership** - Supervises, manages, and/or leads work and workers performing cybersecurity work (i.e., the work described in the Categories and Specialty Area codes with values 10-75). Given that the supervisor oversees individuals with a range of specialty areas, this can encompass multiple various specialty areas.

Click the link to return to "Using the Workforce Framework for Employers"

Assigning the Data Element (Examples)

Below are examples of how position descriptions can be analyzed and linked to an OPM Cybersecurity Data Element. When assigning a code, it is critical for HR representatives, supervisors, and hiring managers to work in a collaborative effort to best determine which code should be used.

Example 1: An employee's duties fall within the work expected of one Specialty Area.

- Job Description Excerpt: "…the employee works on the development of the systems' lifecycle..."
- Data Element: **Code 63, Systems Development**.

Example 2: An employee's duties fall within multiple Specialty Areas in one Category.

- Job Description Excerpt: "…responsible for identification and mitigation of threats to internal information technology (IT) systems or networks, uses defensive measures collected from a variety of sources to identify, analyze, and report events that occur, monitors network to actively remediate unauthorized activities and responds to crisis or urgent situations to mitigate immediate and potential threats..."
- Data Element: **Code 50, Protect and Defend Category**. The category is used since work refers to multiple specialty areas.

Example 3: A manager oversees workers with duties in one Specialty Area.

- Job Description Excerpt: "…oversees workers who develop and write/code new computer applications, software, or specialized utility programs following software assurance best practices..."
- Data Element: **Code 62, Software Assurance and Security Engineering**.

Example 4: A manager oversees workers with duties in multiple Specialty Areas/Categories.

- Job Description Excerpt: "…manages individuals that process tools enabling the organization to identify, document, and access intellectual capital and information content, applies current knowledge of one or more regions, countries, non-state entities, and/or technologies, and supervises, manages, and/or leads work and workers performing cybersecurity work…"
- Data Element: **Code 90, Cybersecurity Supervision, Management and Leadership**. This code is selected because the position is a supervisory one that monitors employees whose work spans over multiple specialty areas (codes 13 and 43).

Systems Operations Professional

Click here to return to the General Cybersecurity Roles main page.

SYSTEMS OPERATIONS PROFESSIONAL

Foundational NIST NICE Specialty Area(s):

Primary Specialty Area(s):	**System Administration (Operate and Maintain)** **Network Services (Operate and Maintain)**
Secondary Specialty Area(s):	***N/A***

Systems Operations Professional: Installs, configures, troubleshoots, and maintains server and systems configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Administers server-based systems, security devices, distributed applications, network storage, messaging, and performs system monitoring. Consults on network, application, and customer service issues to support customer services issues to support computer systems' security and sustainability. Installs, configures, tests, operates, maintains, and manages network devices including hardware, software, and operating systems that permit information sharing across the full spectrum of transmission using all media and to support the security of information and information systems.

Federal Enhancements:

- *Additional enhancements will be established based on Matrix Project SME feedback and CIO Council direction (as applicable)*
- *This role maps to the Systems Operations and Maintenance Professional Workforce Development Matrix published in December 2011 in the "Cybersecurity Workforce Development Matrix Resource Guide." (www.cio.gov – Workforce - Document Library)*

Data Administrator

Click here to return to the General Cybersecurity Roles main page.

DATA ADMINISTRATOR

Foundational NIST NICE Specialty Area(s):

Primary Specialty Area(s):	**Data Administration (Operate and Maintain)**
Secondary Specialty Area(s):	**Knowledge Management (Operate and Maintain)**

Data Administrator: Develops, maintains, administers databases and/or data management systems that allow for the secure storage, query, and utilization of data. Conducts data integration, data modeling, analytic modeling, and data mining.

Federal Enhancements:

- *Additional enhancements will be established based on Matrix Project SME feedback and CIO Council direction (as applicable)*

Computer Network Defense Specialist

Click here to return to the General Cybersecurity Roles main page.

COMPUTER NETWORK DEFENSE SPECIALIST

Foundational NIST NICE Specialty Area(s):

Primary Specialty Area(s):	**Enterprise Network Defense Analysis(Protect and Defend)** **Enterprise Network Defense Infrastructure Support(Protect and Defend)**
Secondary Specialty Area(s):	***N/A***

Computer Network Defense Specialist: Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the enterprise network in order to protect information, information systems, and networks from threats. Tests, implements, deploys, maintains, reviews and administers the infrastructure hardware, software, and documentation that are required to effectively manage the network defense resources. Monitors network to actively remediate unauthorized activities.

Federal Enhancements:

- *Additional enhancements will be established based on Matrix Project SME feedback and CIO Council direction (as applicable)*

Digital Forensics & Incident Response Analyst

Click here to return to the General Cybersecurity Roles main page.

DIGITAL FORENSICS & INCIDENT RESPONSE ANALYST

Foundational NIST NICE Specialty Area(s):

Primary Specialty Area(s):	**Incident Response (Protect and Defend)** **Digital Forensics (Investigate)**
Secondary Specialty Area(s):	**Threat Analysis (Analyze)***

Digital Forensics and Incident Response Analyst: Responds to disruption within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities and evaluates the effectiveness and improvements of existing practices. Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation, and/or criminal, fraud, counterintelligence or law enforcement investigations.

Federal Enhancements:

- The Analyst is responsible for disseminating and reporting cyber-related activities, conducing vulnerability analyses and risk management of computer systems and all applications during all phases of the systems development lifecycle
- *Additional enhancements will be established based on Matrix Project SME feedback and CIO Council direction (as applicable)*

** If adding the Secondary Specialty Area, this role may be considered unique and highly specialized.*

Information Security Auditor

Click here to return to the General Cybersecurity Roles main page.

INFORMATION SECURITY AUDITOR

Foundational NIST NICE Specialty Area(s):

Primary Specialty Area(s):	**Information Assurance (IA) Compliance (Securely Provision)** **Vulnerability Assessment and Management (Protect and Defend)**
Secondary Specialty Area(s):	**Test and Evaluation (Securely Provision)** **Systems Security Analysis (Operate and Maintain)**

Information Security Auditor: Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new and existing information technology (IT) systems meet the organization's information assurance (IA) and security requirements. Ensures appropriate treatment of risk, compliance, and monitoring assurance from internal and external perspectives. Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.

Federal Enhancements:

- The Information Security Auditor is so named to address the reality that these combined specialties may be performed outside of the CIO organization (i.e., Inspector General)
- When performed from an internal perspective, this application may be alternatively know as an Assessor
- The Information Security Auditor relates to the Security Control Assessor defined by NIST SP 800-37. To this end, the IS Auditor is meant to audit the management, operational, and technical security controls of an information system to determine their effectiveness
- *Additional enhancements will be established based on Matrix Project SME feedback and CIO Council direction (as applicable)*

Information Security Architect

Click here to return to the General Cybersecurity Roles main page.

INFORMATION SECURITY ARCHITECT

Foundational NIST NICE Specialty Area(s):

Primary Specialty Area(s):	Systems Security Architecture (Securely Provision) Systems Development (Securely Provision)
Secondary Specialty Area(s):	Information Assurance (IA) Compliance (Securely Provision)

Information Security Architect: Designs and develops system concepts and works on the capabilities phases of the system development lifecycle; translates technology and environmental conditions (e.g., laws, regulations, and best practices) into system and security designs and processes.

Federal Enhancements:

- The Information Security Architect develops security design requirements through sound design methodology, adequate security control application, and effective configuration practices
- The Information Security Architect ensures secure architectural solutions are incorporated into every aspect of the enterprise architecture supporting an organization's key business processes and organizational mission
- The Information Security Architect provides the interface between the Enterprise Architect and the Information System Security Engineering as detailed in NIST SP 800-37
- *Additional enhancements will be established based on Matrix Project SME feedback and CIO Council direction (as applicable*)

Information Systems Security Engineer

Click here to return to the General Cybersecurity Roles main page.

INFORMATION SYSTEMS SECURITY ENGINEER

Foundational NIST NICE Specialty Area(s):

Primary Specialty Area(s):	Systems Security Architecture (Securely Provision) Systems Development (Securely Provision)
Secondary Specialty Area(s):	Test and Evaluation (Securely Provision) Systems Requirements Planning (Securely Provision)

Information Systems Security Engineer: Designs and develops system concepts and works on the capabilities phases of the system development lifecycle; translates technology and environmental conditions (e.g., laws, regulations, and best practices) into system and security designs and processes.

Federal Enhancements:

- The Engineer ensures that security requirements and security engineering practices are incorporated throughout the system development life cycle and engineering maintenance of solutions, applications, products, information systems and network environments to minimize risk to the organization
- Best practices regularly employed by the Information Systems Security Engineer include ensuring adherence to the agency's enterprise architecture, software engineering methodologies, system/security engineering principles, secure design, secure architecture, and secure coding techniques*
- *Additional enhancements will be established based on Matrix Project SME feedback and CIO Council direction (as applicable)*

Information Systems Security Manager

Click here to return to the General Cybersecurity Roles main page.

INFORMATION SYSTEMS SECURITY MANAGER (ISSM)*

** See Information Systems Security Officer (ISSO– these roles vary in organizations – carefully note Federal Enhancements to explain differences.*

Foundational NIST NICE Specialty Area(s):

Primary Specialty Area(s):	**Information Systems Security Officer (Oversee and Govern)**
Secondary Specialty Area(s):	***N/A***

Information Systems Security Manager: Oversees and ensures that the appropriate operational security posture (e.g., network and system security, physical and environmental protection, personnel security, incident handling, security training and awareness) is implemented and maintained for an information system or program. Advises the Authorizing Official, an information system owner, or the CISO on the security of an information system or program.

Federal Enhancements:

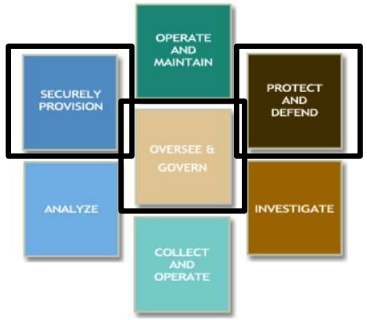
- The ISSM is responsible for the information assurance of a program, organization or enclave
- The ISSM serves as an advocate for all disciplines within the security program including the development and subsequent enforcement of the organization's security awareness programs, business continuity and disaster recovery plans, and all industry and governmental compliance issues
- The ISSM works closely with and in some cases may oversee the ISSO
- In large organizations, the ISSM may be superseded by or report to an IS Program Manager
- *Additional enhancements will be established based on Matrix Project SME feedback and CIO Council direction (as applicable)*

Information Systems Security Officer

Click here to return to the General Cybersecurity Roles main page.

INFORMATION SYSTEMS SECURITY OFFICER (ISSO)*

** See Information Systems Security Manager (ISSM) – these roles vary in organizations – carefully note Federal Enhancements to explain differences.*



Foundational NIST NICE Specialty Area(s):

Primary Specialty Area(s):	**Information Systems Security Officer (Oversee and Govern)**
Secondary Specialty Area(s):	**Information Assurance Compliance (Securely Provision)** **Vulnerability Assessment and Management (Protect and Defend)**

Information Systems Security Officer: Oversees and ensures that the appropriate operational security posture (e.g., network and system security, physical and environmental protection, personnel security, incident handling, security training and awareness) is implemented and maintained for an information system or program. Advises the Authorizing Official, an information system owner, or the CISO on the security of an information system or program.

Federal Enhancements:

- The ISSO communicates with the business at the system level and understands security threats and vulnerabilities to the operations and the system's environment
- The ISSO ensures that the appropriate operational posture is maintained for an information system and is responsible for advising system owners and interfacing with users
- The ISSO will have the technical expertise necessary to oversee the day-to-day security operations of a system and may direct others who manage those operations (e.g., system administrators, database administrators and developers)
- In organizations where the ISSO role is performed by non-government employees, the strategic system decisions are made by the ISSM or CISO
- *Additional enhancements will be established based on Matrix Project SME feedback and CIO Council direction (as applicable)*

Risk and Vulnerability Analyst

Click here to return to the General Cybersecurity Roles main page.

RISK AND VULNERABILITY ANALYST

Foundational NIST NICE Specialty Area(s):

Primary Specialty Area(s):	**Vulnerability Assessment and Management (Protect and Defend)** **Systems Security Analysis (Operate and Maintain)**
Secondary Specialty Area(s):	***N/A***

Risk and Vulnerability Analyst: Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and nonoperational situations. Conducts and documents the systems integration, testing, operations, maintenance and security of an information environment. Coordinates threat and mitigation strategies across the enterprise.

Federal Enhancements:

- This Risk and Vulnerability Analyst adheres to relevant compliance regulations and responds to risk management policies and procedures
- The Risk and Vulnerability Analyst is seen as a key participant in the risk management process as defined by NIST SP 800-37
- *Additional enhancements will be established based on Matrix Project SME feedback and CIO Council direction (as applicable)*

Software Developer

Click here to return to the General Cybersecurity Roles main page.

SOFTWARE DEVELOPER

Foundational NIST NICE Specialty Area(s):

Primary Specialty Area(s):	**Secure Software Engineering(Securely Provision)**
Secondary Specialty Area(s):	***N/A***

Software Developer: Develops and writes/codes new, modifies and enhances existing, and sustains computer applications, software, or specialized utility programs following software assurance best practices throughout the software lifecycles.

Federal Enhancements:

- *Additional enhancements will be established based on Matrix Project SME feedback and CIO Council direction (as applicable)*
- *This role maps to the Information Security Systems and Software Development Professional Workforce Development Matrix published in December 2011 in the "Cybersecurity Workforce Development Matrix Resource Guide." (www.cio.gov – Workforce - Document Library)*

Strategic Planning & Policy Development Professional

Click here to return to the General Cybersecurity Roles main page.

STRATEGIC PLANNING & POLICY DEVELOPMENT PROFESSIONAL

Foundational NIST NICE Specialty Area(s):

Primary Specialty Area(s):	**Strategic Planning and Policy Development (Oversight & Development)**
Secondary Specialty Area(s):	**Legal Advice and Advocacy (Oversight & Development)**

Strategic Planning and Policy Development Professional: Applies technical and organizational knowledge to define an entity's direction, determine resource allocations, establish priorities, and identify programs or infrastructure required to achieve desired goals. Develops policy or advocates for policy change that will support new initiatives or required changes/enhancements.

Federal Enhancements:

- The Strategic Planning & Policy Development Professional also applies knowledge of relevant laws, regulations, guidance and standards to facilitate sound policy development by the organization
- The Strategic Planning & Policy Development Professional develops policy in accordance with internal/organizational requirements as well as external security requirements (e.g., FISMA)
- *Additional enhancements will be established based on Matrix Project SME feedback and CIO Council direction (as applicable)*

Chief Information Security Officer (CISO)

Click here to return to the General Cybersecurity Roles main page.

CHIEF INFORMATION SECURITY OFFICER (CISO)

Foundational NIST NICE Specialty Area(s):

Primary Specialty Area(s):	**Security Program Management (Oversight & Development)**
Secondary Specialty Area(s):	***N/A***

Chief Information Security Officer (CISO): Oversees and manages information security program implementation within the organization or other area of responsibility. This includes strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and/or other resources.

Federal Enhancements:

- The CISO leads the evaluation and assessment of the security program to ensure that all aspects are in compliance with security requirements (e.g., FISMA), while understanding security threats and vulnerabilities to operations and the organization's environment
- In limited cases and in small agencies, the CISO may also assess the management, operational, and technical security controls of the information system to ensure effectiveness
- The CISO is an acknowledged role title at the agency level but the above responsibilities may be fully performed under a different title at the program, sub-agency or component level
- The CISO's authority to carry out the above functions is delegated from the CIO, in accordance with Clinger-Cohen/FISMA requirements
- *Additional enhancements will be established based on Matrix Project SME feedback and CIO Council direction (as applicable)*
- *This role maps to the Systems Operations and Maintenance Professional Workforce Development Matrix published in December 2011 in the "Cybersecurity Workforce Development Matrix Resource Guide." (www.cio.gov – Workforce - Document Library)*